УСТАНОВКА И НАСТРОЙКА PULLEDPORK

PULLEDPORK

- PulledPork – скрипт на Perl, управляющий набором правил для Snort. Может по расписанию загружать последнюю версию правил для COA Snort.

ПОРЯДОК ДЕЙСТВИЙ

1. Подготовка и установка PulledPork
2. Редактирование конфигурационного файла pulledpork.conf
3. Тестовый запуск PulledPork
4. Запуск PulledPork для получения правил snort.rules
5. Редактирование конфигурационного файла snort.conf
6. Проверка корректности файла snort.conf
7. Проверка работы Snort с полученным набором правил

УСТАНОВКА PULLEDPORK*

- Установка пререквизитов:

sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl

* http://c-sec.ru

УСТАНОВКА PULLEDPORK*

- Установка PulledPork:

cd ~/snort_src

wget https://github.com/shirkdog/pulledpork/archive/master.tar.gz -O pulledpork-master.tar.gz

tar xzvf pulledpork-master.tar.gz

cd pulledpork-master/

sudo cp pulledpork.pl /usr/local/bin

sudo chmod +x /usr/local/bin/pulledpork.pl

sudo cp etc/*.conf /etc/snort

* http://c-sec.ru

УСТАНОВКА PULLEDPORK*

- Проверка того, что программа установилась:

/usr/local/bin/pulledpork.pl –V

PulledPork v0.7.3 - Making signature updates great again!

* http://c-sec.ru

РЕДАКТИРОВАНИЕ PULLEDPORK.CONF*

- Строка 19: Ввести свой oinkcode вместо <oinkcode> или закомментировать строку, если нет oinkcode
- Строка 29: Раскомментировать строку #rule_url=https://rules.emergingthreats.net/|emerging.rules.tar.gz|open-nogpl
- Строка 74: Заменить строку rule_path=/usr/local/etc/snort/rules/snort.rules на rule_path=/etc/snort/rules/snort.rules

* http://c-sec.ru

РЕДАКТИРОВАНИЕ PULLEDPORK.CONF*

- Строка 89: Заменить строку local_rules=/usr/local/etc/snort/rules/local.rules на local_rules=/etc/snort/rules/local.rules
- Строка 92: Заменить строку sid_msg=/usr/local/etc/snort/sid-msg.map на sid_msg=/etc/snort/sid-msg.map
- Строка 96: Заменить строку sid_msg_version=1 на sid_msg_version=2

* http://c-sec.ru

РЕДАКТИРОВАНИЕ PULLEDPORK.CONF*

- Строка 119: Заменить строку config_path=/usr/local/etc/snort/snort.conf на config_path=/etc/snort/snort.conf
- Строка 133: Заменить строку distro=FreeBSD-8-1 на distro=Debian-6-0
- Строка 141: Заменить строку black_list=/usr/local/etc/snort/rules/iplists/default.blacklist на black_list=/etc/snort/rules/iplists/black_list.rules
- Строка 150: Заменить строку IPRVersion=/usr/local/etc/snort/rules/iplists на IPRVersion=/etc/snort/rules/iplists

* http://c-sec.ru

ТЕСТОВЫЙ ЗАПУСК PULLEDPORK

- `sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf –l`

```
https://github.com/shirkdog/pulledpork
  _____ ____
 `----,\    )
  `--==\\  /    PulledPork v0.7.3 - Making signature updates great again!
   `--==\\/
 .-~~~~-.Y|\\_  Copyright (C) 2009-2016 JJ Cummings
@_/        /  66\_  cummingsj@gmail.com
|    \   \   _(")
 \   /-| ||'--'  Rules give me wings!
  \_\  \_\\
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

ТЕСТОВЫЙ ЗАПУСК PULLEDPORK

- `sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf –l`

```
https://github.com/shirkdog/pulledpork
  ______ _____
 `----,\    )
  `--==\\  /    PulledPork v0.7.3 - Making signature updates great again!
   `--==\\/
 .-~~~~-.Y|\\_  Copyright (C) 2009-2016 JJ Cummings
@_/        /  66\_  cummingsj@gmail.com
|    \   \   _(")
 \   /-| ||'--'  Rules give me wings!
  \_\  \_\\
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

ЗАГРУЗКА ПРАВИЛ С ПОМОЩЬЮ PULLEDPORK

- sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf –I –P

В каталоге etc/snort/rules должен появиться файл *.rules

(по умолчанию snort.rules)

РЕДАКТИРОВАНИЕ SNORT.CONF

- Для того, чтобы snort учитывал загруженные правила, требуется раскомментировать строку
- include $RULE_PATH/snort.rules

ПРОВЕРКА КОРРЕКТНОСТИ КОНФИГУРАЦИИ

- После добавления строки с правилами следует запустить snort с ключом проверки конфигурационного файла:

- sudo snort -T -c /etc/snort/snort.conf -i eth0

ТЕСТОВЫЙ ЗАПУСК SNORT

- После проверки конфигурации Snort следует запустить программу с новым набором правил и добиться хотя бы одного срабатывания правил из набора